

FILED ENTERED
LOGGED RECEIVED
IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
AUG 02 2017

IN THE MATTER OF THE SEARCH OF:

14613 CAMBRIDGE DR.
UPPER MARLBORO, MD 20772
AND ELECTRONIC STORAGE DEVICES
THEREIN

AT GREENBELT
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND

BY

Case No.

Filed Under Seal

TMD 17-01962

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jason R. Bell, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Lieutenant with the United States Capitol Police (the "USCP"), where I have served since April 7, 2002. I am currently assigned to the Investigations Division. I have attended the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. I have received training and gained experience in search warrant applications, the executions of searches and seizures, computer crimes, computer evidence identification, computer evidence seizure and processing, and various other relevant training.

2. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2261A(2)(B) (Cyberstalking), 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. 1512(c) (Obstruction of Justice), and 18 U.S.C. §1001(a)(2) (False Statements) have been committed. Section 18 U.S.C. § 2261A(2)(B), in relevant part, imposes criminal penalties on whoever uses any interactive computer service or

TMD

JB
7/15/17

electronic communication service or system of interstate commerce with the intent to harass or intimidate to engage in a course of conduct that causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person. Section 18 U.S.C. § 371, imposes criminal penalties if two or more persons conspire to commit an offense against the United States, and one or more of such persons do any act to effect the object of the conspiracy. Section 18 U.S.C. §1512(c), in relevant part, imposes criminal penalties on persons who corruptly obstruct justice in an official proceeding, which includes a grand jury investigation. 18 U.S.C. § 1001(a)(2), in relevant part, imposes criminal penalties on whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully makes a materially false, fictitious, or fraudulent statement or representation. Based on your affiant's investigation into these violations, there is probable cause to search the location described in Attachment A (that is, the "PREMISES" located at 14613 Cambridge Drive, Upper Marlboro, MD 20772) for evidence of these crimes further described in Attachment B.

JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because it your affiant has probable cause to believe the property is located in the District of Maryland. *See, e.g.*, Federal Rule of Criminal Procedure 41(b).

PROBABLE CAUSE

Private Images of Delegate and Family Were Distributed Through Hotmail and Facebook

5. The USCP has been investigating allegations that unknown person/persons intentionally accessed the cell phone and/or computers of SP, a U.S. Delegate to the House of Representatives from the Virgin Islands and/or its spouse, JBS, either without authorization or



exceeding their authorization; information was taken from these devices and has been disseminated through the internet in an apparent effort to cause substantial emotional distress. SP works in the District of Columbia, and the SP's electronic devices are regularly located in the District of Columbia.

6. As part of this investigation, I have obtained an email that was sent from the email account the3kingz@hotmail.com by an individual or individuals using the pseudonym "Susan Ricenville" to a former delegate from the Virgin Islands, on or about July 2, 2016. The email contained the subject line "Luk Whoo Leadin We: No Wonda Dis Whole Territory Screw Up". The email stated the following: "Wha De Hell Dey Exposin Dis Lil Gul To? Luk Close. Me No Vote Fah She!!!! Sen 2 Human Services." The email contained a video taken by SP on her cell phone in the privacy of her residence. The video was a private recording of images of SP, JBS, and their daughter in the home's bathroom.

7. On or about July 6, 2016, an online news media source in the Virgin Islands received a similar email from "Susan Ricenville the3kingz@hotmail.com," containing subject line "Luk Whoo Leadin We: No Wonda Dis Whole Territory Screw Up – Plaskett MuSt GO!". The message stated "Luk Close. Wha de hell day exposing dis lil gul to?" The owner of the online news media source stated the video depicted an adult black male, a juvenile, and a female voice, which he identified as SP.

8. On or about July 8, 2016, another individual located in the District of Columbia reported receiving a similar email from "Susan Ricenville the3kingz@hotmail.com," containing subject line "Luk Whoo Leadin We: No Wonda Dis Whole Territory Screw Up-Plaskett MuSt GO!". The email stated "Luk Close. Wha de hell day exposing dis lil guy to – Stacey filmed ah dis? Department Human Services mus kno." The email contained video of SP, her husband and



daughter, as well as a nude topless photo of SP. The individual also stated that after receiving the email he received a "friend" request from a Facebook user with the account name "Susan Ricenville". The individual stated it does not know a "Susan Ricenville," and did not accept the friend request.

9. On or about July 21, 2016, SP provided your affiant a screenshot of the Facebook account for a community page for residents of St. Thomas. The screenshot was taken on July 21, 2016. In the screenshot, the private video of SP's husband can be seen on the community Facebook page. The screenshot shows the video was posted by Facebook account "Susan Ricenville". The comment above the video stated "Dey took it down but dis [SP] recordin she husband wah da little gurl watchin dat necked man. Dis is screw up!"

10. Your Affiant interviewed SP who stated that it had received notification regarding the emails containing the video of its spouse from a former Virgin Islands Delegate who had received the email. SP viewed the video contained in the email and the Facebook posting, and identified it as a personal video that SP took with family members in their home, and the photographs as digital images that were taken by SP. SP indicated that the video was a personal video that was taken on SP's personal cellular phone, and that the photographs were images taken with the same cellular phone. SP indicated the video was private, and that SP did not recall ever sending the video to any other person, and that SP never gave permission for anyone to have or distribute this video or any other personal image from this device. SP indicated that the photographs distributed by the "Susan Ricenville" Facebook account were also private in that the images were only shared via text message with JBS. Both JBS and SP confirmed they did not share these images or video with others, nor did they authorize their dissemination or



distribution. After learning of the emails and Facebook postings from “Susan Ricenville,” SP notified her attorney, and others.

Investigation Reveals that Juan McCullum Is Involved in Distributing Images

11. As part of this investigation, the Government submitted a subpoena to Facebook for the user account “Susan Ricenville” on July 26, 2016. On August 4, 2016, the Honorable Deborah Robinson also signed a search warrant for the “Susan Ricenville” Facebook account. Your affiant served the warrant on Facebook that same day.

12. On August 11, 2016, in response to the subpoena, Facebook provided certain transactional records. The records show that “Susan Ricenville” registered the Facebook account on July 17, 2016. The records also reveal that the Facebook Account was registered from an Internet Protocol (IP) address: 2601:14d:8400:64a0:e4ba:eeec:be6b:165f. Your affiant has learned that this Facebook IP address is assigned by Comcast.

13. On August 12, 2016, the Government submitted a subpoena to Comcast for subscriber information of the IP address provided by Facebook. On August 16, 2016, in response to the subpoena, Comcast provided information showing that Juan MCCULLUM is the subscriber and listed his address as 400 M St SE, Apt 424, Washington, DC. The Comcast records show that the account service began on January 16, 2014, and is currently an active account. MCCULLUM has self-identified this address as his home address in employment paperwork that he has provided for the U.S. House of Representatives.

14. On September 13, 2016, a search warrant was executed at 400 M St SE, Apt 424, the confirmed residence for MCCULLUM. Multiple electronic devices were recovered from the premises, including an Apple iMac desktop computer recovered from the kitchen counter. When officers arrived at the residence, MCCULLUM and another individual, Malik Bland, were



present. Each consented to a voluntary interview. Both individuals were asked to identify the owner of the Apple iMac desktop computer on the kitchen counter. Both individuals indicated that they did not know who owned it. A preliminary extraction of data from the Apple iMac computer revealed multiple personal photos belonging to SP under an account on the computer named "Uncle BB." Included among these images were the same private SP and JBS videos and images which were sent through the 3kingz@hotmail.com account and the "Susan Ricenville" Facebook accounts. Other private photographs and videos of SP and JBS, including naked and sexual images belonging to SP and JBS ("Other SP Images"), were also found on the Apple iMac computer. Photographs of McCullum's identification and a check in the name of MCCULLUM dated April 20, 2015, were also found within the "Uncle BB" account in the Apple iMac computer.

15. Your affiant interviewed SP who stated that MCCULLUM was previously employed as staff to its Congressional Office until June 10, 2016. SP further stated that in March 2016, SP's iPhone was not functioning properly. MCCULLUM told SP that he had a friend "Malik" who worked at Apple, and he agreed to take the device to his friend for repairs. SP stated that it gave its phone to MCCULLUM so he could have the device repaired. SP provided a screen shot of a text message from MCCULLUM on Tuesday, March 22, 2016; "Hey Boss - Malik wants me to bring your phone in tomorrow at noon replacement". SP stated that it remembers MCCULLUM calling SP while he was at the Apple store, for the iPhone's password, so his friend could access the device. SP stated that later MCCULLUM returned the repaired iPhone and stated that the problems with the device were due to sand from the beach. The iPhone SP provided to MCCULLUM contained the images and personal video that were later disseminated by the 3kingz@hotmail.com and Susan Ricenville Facebook accounts. Your



JB
7/13/17

affiant has also confirmed that the Other SP Images were also located on SP's iPhone and the neither SP nor JBS has authorized or consented to the copying or distribution of these images. Neither JBS nor SP provided consent or authorization to MCCULLUM or his friend to copy the device or take or download any images from the device.

MCCULLUM Communicated with Dorene Browne-Louis about the Images

16. A forensic exam was conducted of MCCULLUM's Apple iPhone 6 device recovered from the premises search warrant. A review of the contacts listed on the device show the name "Debbie Lloyd" associated with the phone number "340-690-2254". Phone number "340-690-2254" belongs to Dorene BROWNE-LOUIS (hereafter, "DBL"). Your affiant has communicated with DBL on this phone number and DBL confirmed that this number belonged to her in July, 2016. The forensic exam of McCullum's Apple iPhone 6 device revealed a text conversation on July 20, 2016, between MCCULLUM and DBL:

- MCCULLUM "Somebody talking about it"
- [MCCULLUM then texted a photograph of a Facebook user comment (Ak Karam) referencing a number of news items including a sex tape in the Virgin Islands]
- DBL "Talking about what"
- MCCULLUM "Click pic"
- DBL "Don't See..."
- DBL "Talking bout when to eat"
- MCCULLUM "Lol"
- MCCULLUM "Read AK Karam post"
- DBL "Awww, but no name"



JB
7/13/17

- MCCULLUM “Yeah-it’s coming....All brewing”
- DBL “Awww”
- MCCULLUM “Susan Ricenville has made many a friends on FB
[message included three emojis of the see no evil, hear no evil monkeys]”
- DBL [Responds with an emoji of a hear no evil monkey]

17. Your affiant interviewed W1, who stated that MCCULLUM was close friends with SP’s former scheduler DBL. Your affiant is aware through information gathered from forensic examinations of DBL’s phone and interviews of witnesses, that DBL was looking for new employment as early as December 2015 and DBL resigned from SP’s office at or about the end of March 2016. During an interview with SP, SP indicated to your affiant that it saw MCCULLUM at DBL’s residence on August 17, 2016, during a small gathering due to the death of DBL’s spouse. Through multiple witness interviews, and forensic exams of DBL’s device, your affiant is also aware that DBL and MCCULLUM regularly met in-person and corresponded with one another through phone, messaging and the internet.

18. On October 12, 2016, in response to a search warrant signed by the Honorable Deborah Robinson, Microsoft provided account information for the3kingz@hotmail.com. Included in the information provided by Microsoft were the sent and received messages and emails, which included the email addresses of persons who were sent messages, as well as images and videos included in those messages. The return indicated that the email account was used and accessed between July 2, 2016 and July 24, 2016, and that the account sent numerous email messages with private and nude SP and JBS images using the alias “Susan Ricenville” to numerous persons, including media outlets and well-known persons in the Virgin Islands political community. Additional information provided by Microsoft about the



JB
7/13/17

3kingz@hotmail.com indicated that the account was created by, and logged into, using a number of IP addresses belonging to three different providers: Comcast, Verizon Wireless and the U.S. House of Representatives. Further legal process to Comcast and Verizon Wireless confirmed the following: the Comcast IP addresses were owned by users in the 900 block of Tyler Street, in Pearl, Mississippi, and by Juan McCullum of 400 M Street, SE, Apt. 424, Washington, D.C., and the Verizon Wireless IP addressed belonged to Juan McCullum's work iPhone which had been provided by his new employer at the U.S. House of Representatives. The Comcast IP addresses in Mississippi were used to access the 3kingz@hotmail.com account between July 2 and July 13th. Your affiant has confirmed through this investigation that MCCULLUM was visiting family members in the 900 block of Tyler Street in Pearl, Mississippi during this period of time. Your affiant has also confirmed that MCCULLUM was in the District of Columbia when the IP addresses resolving to Comcast account at the 400 M Street, S.E. apartment and the House of Representatives were being used. Based on the foregoing, your affiant believes there is probable cause to believe that MCCULLUM owned and controlled the 3kingz@hotmail.com email address during the period of time that the account was active in distributing private SP and JBS photographs and video, including naked images, to numerous persons through the internet without authorization.

19. The Microsoft search warrant response for the 3kingz@hotmail.com account confirms that MCCULLUM sent email account dpblouis@gmail.com three emails, both directly and blind copied (bcc), which included SP and JBS private images which had been taken and distributed without permission. Your affiant knows that dpblouis@gmail.com is listed as the contact email for "Dorene Louis", in SP's device. On November 15, 2016, in response to a legal



request, GOOGLE provided subscriber information for user account dpblouis@gmail.com. The subscriber listed for the account is "Dorene Louis."

November 9 and 23, 2016 Interviews of DBL

20. On November 9, 2016, your affiant interviewed DBL at her residence located in Upper Marlboro, MD (14613 Cambridge Drive). She stated that she received an email from "Susan Somebody", which contained a topless photo of SP. DBL identified her email address as dpblouis@gmail.com. DBL stated that once she viewed the photo she notified SP via text message and may have forwarded the email to her former chief of staff. DBL stated that she heard first about the photo leak from people in the Virgin Islands who called her believing she still worked for SP.

21. On November 22, 2016, DBL was interviewed by your affiant and Assistant U.S. Attorneys. DBL was shown the July 20, 2016 text conversation with MCCULLUM described in paragraph 17, and she denied having the conversation. DBL denied knowing about the persons or individuals responsible for the distribution of the private SP images, and she denied knowing that MCCULLUM had anything to do with their distribution. DBL acknowledged receiving a number of SP's private images, but she denied sending, forwarding or distributing the messages or private images of SP onto any person other than to SP's agents to inform SP about the distribution of these images. DBL also denied that she deleted any text messages or emails with MCCULLUM from her phone, or any information that related to the SP images. DBL thereafter consented to a forensic examination to be conducted on her cell phone.

Communications Between MCCULLUM and DBL, Including on DBL's Phone



22. The forensic examination of DBL's phone indicated a number of communications and text messages with MCCULLUM during the period of the distribution of the SP's private images through the 3kingz@hotmail.com and "Susan Ricenville" Facebook accounts. For example, on July 2, 2016, the Microsoft returns indicate that after the 3kingz@hotmail.com account was set up, the first email sent by the account included private and naked SP and JBS images, and was directed to three persons, including "kenn.mapp@aol.com." Kenneth E. Mapp was and is the sitting Governor of the Virgin Islands. According to the Microsoft records, the email bounced back from the "kenn.mapp@aol.com" email address to the 3kingz@hotmail.com account at 08:38 GMT on July 2, 2016. The DBL phone forensics indicate that at 08:41 GMT on July 2, 2016, MCCULLUM texted DBL twice: "One bounce back," and "K.M." Based on the timing of these text messages your affiant believes the reference to "K.M." in the text messages is to Kenneth Mapp. The DBL phone forensics also indicated that both text messages had been "deleted" by the user of the phone. The DBL phone forensics indicate there was a telephone call between MCCULLUM and DBL lasting almost two minutes starting at 14:44 GMT on July 2, 2016. At 15:11 GMT on July 2, 2016, the 3kingz@hotmail.com account resent the original message to "ken.mapp@aol.com". The Microsoft records do not include any bounce back from the message sent to this new email account. The DBL phone forensics also indicate there were three at least two additional phone calls between MCCULLUM and DBL on July 2, 2016 (at 19:40 GMT for more than 2 minutes, 19:50 GMT for more than 2 minutes, and an apparent attempted call at 21:16 GMT).

23. Additionally, the Microsoft return for the 3kingz@hotmail.com account indicated that on July 6, 2016 at 16:40 GMT, the account forwarded private SP and JBS images to several news media outlets. DBL's phone forensics indicate that on July 6, 2016 at 21:04 GMT



JB
7/3/17

MCCULLUM texted DBL "Somebody will pay for how we were treated." The DBL phone forensics indicate that the text message had been deleted by the user of the phone.

24. The Microsoft return for the 3kingz@hotmail.com account indicated that three emails were sent by the account with private and naked SP images directly to dpblouis@gmail.com on July 8, 2016 at 00:37, 00:48 and 01:10 GMT. The DBL phone forensics indicate there were at least two phone calls between DBL and MCCULLUM, one at July 7, 2016 at 23:40 GMT for more than 14 minutes, and a second call at July 8, 2016 at 00:56 GMT for more than 5 minutes.

DBL Reports a Missing iPad

25. On November 23, 2016, DBL contacted your affiant, and stated that she wanted to report that she had a missing iPad device that was linked to her cell phone. She stated that MCCULLUM had borrowed this device, and had not returned the device. She provided this a possible reason why she did not recognize the text messages between her and MCCULLUM, and suggested that perhaps MCCULLUM was using the device to conduct his criminal activities, including texts sent to her cell phone. Your affiant is aware that the term "iPad" is sometimes used to refer to any electronic tablet device that can access the internet.

Images Were Also Distributed Through BENNETTRN2001@YAHOO.COM Account

26. As part of the investigation your affiant interviewed W2 on February 24, 2017 with Assistant U.S. Attorneys. W2 is a subject of this investigation who received several private SP images from the 3kingz@hotmail.com account in July 2016. In July 2016, W2 was in an intimate relationship with DBL and assisting SP's competitor in the contested Democratic Party Primary in July 2016. W2 confirmed that it spoke with DBL about the images in July 2016, and that DBL and a person identified as "Susan Ricenville" forwarded W2 private images of SP to



JB
7/13/17

W2 via email in July 2016. W2 indicated the account which was used to receive the images was "bennetttrn2001@yahoo.com." W2 indicated it forwarded the SP and JBS private images using this same email address to at least one other person. In an initial interview with your affiant on February 8, 2017, W2 denied that it had distributed or forwarded any SP private images to any person. Your affiant is also aware that DBL was in close contact with W2 in July 2016. For example, your affiant is aware that DBL phone forensics indicate that DBL was communicating via phone with W2 on July 7, 2016, immediately before and after talking with MCCULLUM; the phone records indicate a phone call between DBL and W2 of more than 2 minutes on July 8, 2016 at 00:54 GMT and of 50 seconds at 01:30 GMT. Your affiant is also aware that the phone forensics indicate that W2 spoke with DBL on July 2, 2016 near in time to communicating with MCCULLUM, including at 19:32 GMT for more than 7 minutes, at 19:43 GMT for more than 4 minutes, and 21:11 GMT for more than 4 minutes). The Microsoft returns of the 3kingz@hotmail.com account confirm that at least four emails containing private and naked SP images were sent to W2's email address of "bennetttrn2001@yahoo.com" between July 2 and July 20, 2016.

27. As discussed in greater detail immediately below, your Affiant is aware DBL has had ongoing communications and discussions about this investigation with SP, MCCULLUM and W2. Indeed, the forensic examination of DBL's phone indicates she has had specific electronic communications about the status of the investigation, including discussion about testimony before the Grand Jury, with MCCULLUM, W2 and others.

Obstruction of Justice

28. Between on or about November 8, 2016, and on or about November 22, 2016, your affiant and other members of law enforcement interviewed DBL on multiple occasions.



JB
7/13/17

During these interviews, DBL made numerous false and misleading statements about her knowledge of MCCULLUM's activities, including MCCULLUM's use of the Susan Ricenville Hotmail and Facebook accounts. In these interviews, DBL falsely told federal law enforcement officers, among other things, that she did not know that MCCULLUM was involved in the distribution of images related to Delegate S.P. and that she did not delete messages on her cellular phone related to MCCULLUM or Delegate S.P.

29. On or about November 22, 2016, DBL testified before a federal grand jury empaneled in the District of Columbia about MCCULLUM and her knowledge of his distribution of the Nude Images and Videos in July 2016. DBL provided false, incomplete, and misleading testimony to the federal grand jury about DBL and her knowledge of his distribution of the Nude Images and Videos. These false and misleading statements included, but were not limited to: (1) that DBL did not have any discussion with MCCULLUM about the Nude Images and Videos prior to receiving the material by email from "Susan Ricenville"; (2) that DBL was unaware of who was responsible for distributing the Nude Images and Videos; (3) that DBL did not know who was using the name "Susan Ricenville"; and (4) that DBL did not know that MCCULLUM wanted to seek revenge against Delegate S.P.

30. Evidence of DBL's obstruction includes the aforementioned communications with MCCULLUM revealed in a forensic examination of DBL's phone, included deleted communications, as described above.

Indictment and Arrest of DBL

31. On July 11, 2017, a federal Grand Jury sitting in the District of Columbia indicted MCCULLUM and DBL; MCCULLUM was charged with two counts of felony Cyberstalking, and DBL was charged with two counts of Obstruction of Justice. The case number is 17-CR-131



JB
7/17/17

(JDB). The Federal District Court for the District of Columbia issued an arrest warrant on July 11, 2017, for DBL and MCCULLUM based on this indictment.

32. On July 12, 2017, USCP Special Agents arrested DBL at her place of employment, located at 1331 F. St. NW Washington, DC. DBL was transported to 119 D St. NE (US Capitol Police Headquarters) where she was processed and an interview was conducted.

33. Prior to conducting the interview, Special Agent Lawrence Anyaso and your affiant advised DBL of her Miranda rights. DBL waived her rights and voluntarily agreed to be questioned by the agents.

34. During the interview, your affiant asked DBL about her iPad that she previous stated was missing on November 23, 2016. DBL stated that in April 2017, she located the missing iPad at her residence located at 14613 Cambridge Dr. Upper Marlboro, MD 20772. DBL further stated that the iPad is currently at her residence. DBL stated that she believed she and MCCULLUM had access to the iPad and used the device prior to the device being lost in late 2016. DBL stated that she has not deleted anything from the iPad since she has found the device. Furthermore DBL provided your affiant with the password for the device. When asked to provide consent to search the device she declined to provide consent.

35. Your affiant is aware that DBL has resided at 14613 Cambridge Drive, Upper Marlboro, MD for more than a year. She has self-identified this address to law enforcement and her former employers. Your affiant has also interviewed DBL at the residence and been inside the property. The property is as a single story single family residence with basement, a gray roof, white siding, and reddish-brown brick siding on the front right of the residence as you view it from Cambridge Dr.

JB
7/13/17

36. Based on your affiant's experience and training, because DBL has indicated (as described above) that a tablet device was linked to DBL's cell phone or controlled by MCCULLUM, the tablet is likely to contain records of illegal activity, including the communications between DBL and MCCULLUM that were revealed in a forensic examination of DBL's cell phone. That is, the "linking" of the two devices means that copies of communications on one device may be present on the other. Similarly, just as communications (or portions thereof) that had been deleted (or attempted to be deleted) were able to be recovered by a forensic examination of DBL's cellular phone, those communications and related ones may still be present on the iPad, including additional related data, such as who used the iPad at or about the time of those communications between DBL and MCCULLUM.

37. Based on the above, your affiant believes there is probable cause to believe that one or more devices inside the PREMISES, including electronic devices that may be physically on or with persons inside the PREMISES, will contain documents, data, electronic evidence and/or unique digital signatures which contain evidence of the crimes under investigation.

TECHNICAL TERMS

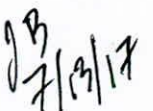
38. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

- a. "Computer" means "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." See 18 U.S.C. § 1030(e)(1).



JB
7/13/17

- b. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- c. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.
- d. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work.



Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

- e. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- f. The Internet is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- g. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"),



JB
7/13/17

cable, dedicated circuits, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name - a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

- h. "Internet Connection" means a connection required for access to the Internet. The connection would be provided by cable, DSL (Digital Subscriber Line), wireless, or satellite systems.
- i. A "modem" translates signals for physical transmission to and from the Internet Service Provider, which then sends and receives the information to and from other computers connected to the Internet.
- j. A "router" often serves as a wireless access point and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. The router is in turn typically connected to a modem.
- k. "Domain Name" means the common, easy-to-remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are



89
7/19/17

typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

- l. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Markup Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- m. “Cache” means the text, image, and graphic files sent to and temporarily stored by a user’s computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website.
- n. “Secure Hash Algorithm Version 1 hash value” (SHA 1 hash value) is an algorithm that processes digital files, resulting in a 160-bit value that is unique to that file. It is computationally infeasible for two files with different content to have the same SHA 1 hash value. By comparing the hash values of files, it can be



JB
7/13/17

concluded that two files that share the same hash value are identical with a precision that exceeds 99.9999 percent certainty. There is, for example, no known instance of two different child pornographic images or videos having the same SHA1 hash value.

- o. "Peer to Peer file sharing" (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to set up files on a computer to be shared with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user's computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network. However, a tool used by law enforcement restricts the download so that the file is downloaded, in whole or in part, from a single user on the network. When a user wishes to share a file, the user adds the file to his a shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's SHA 1 has value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value. Third party software is available to identify the IP address of a P2P




28
7/13/17

computer that is sending a file. Such software monitors and logs Internet and local network traffic.

- p. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

- q. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

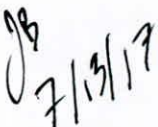


- r. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.
- s. A "botnet" is a collection of compromised computers, known as "bots," that autonomously respond to and execute commands issued by the botnet's owner, often for nefarious purposes. Computers become part of a botnet by being infected with malware, which may install itself on a user's computer without the user's knowledge, often by taking advantage of web browser vulnerabilities or by tricking the user into running a Trojan horse program. Once the computer is infected and becomes a bot in the botnet, the malware can listen for, respond to, and execute commands issued by the botnet's owner, for example, to send out spam e-mail or to make connections to a particular server as part of a distributed denial of service, or "DDoS," attack, defined below.
- t. "Carding" is an activity in which a perpetrator steals or traffics in stolen credit card information or uses stolen credit card data to buy goods and services.
- u. A Distributed Denial of Service, or "DDoS," attack on a server refers to the process of making massive requests to a particular server or domain. The number of requests to a domain, server, or IP address eventually overwhelms the target, and causes it to stop functioning.
- v. Twitter is an online social networking service and microblogging service that enables its users to send and read text-based messages of up to 140 characters,



known as “tweets.” Tweets are publicly visible by default, but senders can restrict message delivery to just their followers. Users can tweet via the Twitter website, compatible external applications (such as for smartphones), or by Short Message Service (SMS), a text messaging service component of phone, web, or mobile communication systems.

- w. “PDA”: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- x. “Tablet”: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those



functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

y. “Wireless telephone or device: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

z. “Portable media player”: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital



JB
7/13/17

data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

39. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or on other electronic storage media or digital devices. As used herein, the terms "electronic storage media" and "digital devices" include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of electronic storage media and digital devices or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

40. *Probable Cause.* Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that if electronic storage media or digital



JB
7/13/17

devices are found on the PREMISES, there is probable cause to believe that the records and information described in Attachment B will be stored in the electronic storage media and digital devices for at least the following reasons:

- a. Individuals who engage in online criminal activity and utilize mobile phones and devices, including those who violate 18 U.S.C. §2261A(2)(B) (Cyberstalking), and 18 U.S.C. §1512 (Obstruction of Justice), not only use computers and other electronic devices to access websites used for illegal activity and to communicate with co-conspirators online, but also store on computer hard drives and other electronic storage media documents and records relating to their illegal activity. Online criminals store these documents and records, which can include logs of online “chats” with co-conspirators; email correspondence; contact information of co-conspirators, including telephone numbers, email addresses, identifier for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things, (1) keep track of co-conspirator's contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators; and (4) store stolen data for future exploitation.
- b. Individuals who engage in the foregoing criminal activity, in the event that they change computers, will often “back up” or transfer files from their old computers’



hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

- c. Computer, smart phone, and other digital device files, or remnants of such files, can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to an electronic storage medium can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device such as a home computer or a smart phone, the data contained in the file does not actually disappear; rather, that data remains on the electronic storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the electronic storage medium that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from an electronic storage medium depends less on when the file



83
7/27/17

was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

d. *Forensic Evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence or information that establishes how electronic storage media or digital devices were used, the purpose of their use, who used them, and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be on electronic storage media and digital devices in the PREMISES because:

- i. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data on the electronic



JB
7/13/17

storage media not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

- ii. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address



JB
7/13/17

books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- iii. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- iv. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic storage media and digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on electronic storage media or digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- v. Further, in finding evidence of how electronic storage media or a digital device was used, the purpose of its use, who used it, and when, sometimes



JB
7/13/17

it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

- vi. I know that when an individual uses a digital device to attempt to disseminate stolen images anonymously, or to obstruct justice, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

41. *Methods To Be Used To Search Digital Devices.* Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

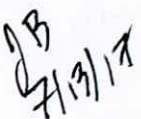
- a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time. There



JB
7/17/17

are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals, specialized equipment, and software programs necessary to conduct a thorough search. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

- b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from electronic storage media also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.
- c. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises. Smart phones capable of storing 64 gigabytes, flash drives capable of storing 128 gigabytes, and desktop computers capable of storing 500 or more



gigabytes are now commonplace. Consequently, just one device might contain enormous amounts of data.

- d. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.
- e. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous

TMD

89
7/13/17

modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

- f. Analyzing the contents of mobile devices can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even



older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, “Hide It Pro,” disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

42. Based on all of the foregoing, I respectfully submit that searching any electronic storage media or digital device for the information, records, or evidence subject to seizure pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the media or devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.



JB
7/13/17

43. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

- a. Upon securing the PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any electronic tablets (such as any iPads), as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such electronic storage media or digital devices at the PREMISES. The electronic storage media and digital devices, and/or any digital images thereof created by law enforcement in aid of the examination and review, will be examined and reviewed by law enforcement personnel in order to extract and seize the information, records, or evidence described in Attachment B.
- b. The analysis of the contents of any seized electronic storage media or digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and



JB
7/13/17

possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

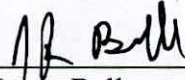
- c. In searching the seized electronic storage media or digital devices, the forensic examiners may examine as much of the contents of the electronic storage media or digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized electronic storage media or digital devices will be specifically chosen to identify only the specific items to be seized under this warrant.

CONCLUSION

44. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.



Respectfully submitted,



Jason Bell
Lieutenant
United States Capitol Police

Subscribed and sworn to before me
on July 13, 2017 :

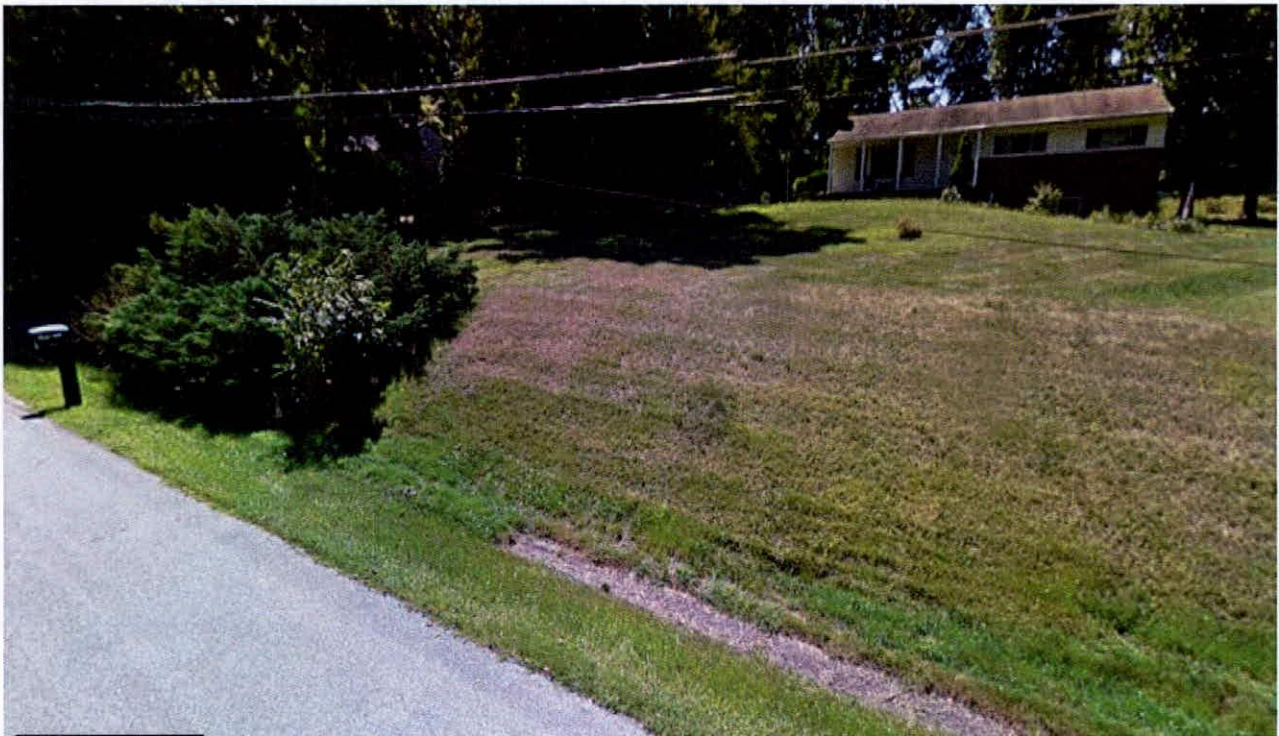


UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED

The property to be searched is **14613 Cambridge Drive, Upper Marlboro, MD 20772**, further described as a single story single family residence with basement, a gray roof, white siding, and reddish-brown brick siding on the front right of the residence as you view it from Cambridge Dr. The residence has a driveway on the left side of the property when facing the front of the residence. A green mailbox displaying the numbers "14613" is located at the end of the residence driveway.



mm

ATTACHMENT B

ITEMS TO BE SEIZED

- A. Any tablet device capable of storing electronic data or accessing the internet, including any iPad devices.
- B. All evidence, fruits, and instrumentalities stored in the premises, related to violations of 18 U.S.C. § 2261A(2)(B) (Cyberstalking), 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. 1512(c) (Obstruction of Justice), and 18 U.S.C. 1001(a)(2) (False Statements), including but not limited to:
 - 1. Records and information, and items related to violations of the aforementioned statutes;
 - 2. Records, information, and items related to the identity of Juan R. McCullum and DBL;
 - 3. Records, information, and items related to DBL's relationship with McCullum or SP;
 - 4. Records, information, and items related to any access to or dissemination of SP or JBS's private images;
 - 5. Records, information, and items related to the state of mind of McCullum, DBL or any individuals seeking to access or disseminate private images of SP or JBS;
 - 6. Records, information, and items related to email account the3kingz@hotmail.com ("the Hotmail account") or the Facebook account of "Susan Ricenville" ("the Facebook account");
 - 7. Records, information, and items related to any associates of McCullum or other individuals he communicated with about his plans to access or disseminate private images of SP or JBS;
 - 8. Records, information, and items indicating how and when the Hotmail account and/or the Facebook account was created, accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
 - 9. Records, information, and items related to the possession of the private images of SP and JBS;



JB
7/13/17

10. Records, information, and items related to any attempt to intimidate or harass SP, including emails sent or received;
11. Records, information, and items related to who communicated with the Hotmail or Facebook account, including records that help reveal the identity and whereabouts of such person(s);
12. Records, information, and items that discuss or relate to the identity of occupants, visitors or residents of the apartment, including lease paperwork, identification information, and mail matter;
13. Records, information, and items relating to the identity of persons who had access to any electronic devices seized during the investigation;
14. Records, information, and items relating to the means and source of payment for email, computer, and/or internet services (including any credit card or bank account number or digital money transfer account information);
15. Records, information, and items related to the identity of any co-conspirators or aiders and abettors, including records that help reveal their whereabouts;
16. Records, information, and items related to the operation of a botnet;
17. Records, information, and items related to the identity or location of the suspects, or storage facilities or places which may also contain evidence of these crimes;
18. All records or material relating to passwords which may be used on any electronic devices seized; and
19. Any communications or records, deleted or otherwise, involving McCullum, his devices, or any alias accounts from January 1, 2016 to present.

All digital evidence, as that term is used herein, means the following:

- (a) Any computer equipment or digital devices that are capable of being used to commit or further the crimes referenced above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes, including central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices including paging devices and cellular telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communication devices



JB
7/13/17

such as modems, routers, cables, and connections; storage media; and security devices;

- (b) Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes referenced above, or to create, access, process, or store evidence, contraband, fruits, or instrumentalities of such crimes;
- (c) Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes referenced above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes;
- (d) Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;
- (e) Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;
- (f) Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;
- (g) Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and
- (h) All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during the time the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.



DIGITAL EVIDENCE SEARCH PROCEDURE [if necessary]

In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

(Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant. As part of its forensic examination, law enforcement may further remove any electronic device or image of such device from this jurisdiction to another jurisdiction for the purposes of continuing its forensic review.

If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

(If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its



JB
7/13/17

owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

A handwritten signature in blue ink, consisting of a series of loops and a long horizontal stroke.

83
7/13/17